International Journal of
Technology and Emerging Research
ISSN: 3068-109X (online) | ISSN: 3068-1995 (print) | https://www.ioro.org/ijter

International Conference on Intelligent Technologies for Tomorrow (ICITT-2026) · 18 August 2026

Image Steganography Under Multiple Performance Metrics: A Comparative Study

Nisha C D [1], Dr.Thomas monoth

[1] *Research Scholar, Department of Computer Science, Mary Matha Arts and Science College, Kannur University, Wayanad,Mananthavady, Kerala, 670645 & Asst.Professor ,Department of Computer Science,Little Flower College(autonomous) Guruvayur,Kerala,680103.*

[2] *Department of Computer Science, Mary Matha Arts and Science College, Kannur University, Wayanad, Mananthavady, Kerala 670645.* ***Corresponding author:*** *nisha@littleflowercollege.edu.in*

Abstract

Image steganography performance depends on a trade-off among embedding capacity, imperceptibility, structural fidelity, robustness, security, and computational cost. This paper presents a comparative evaluation framework for spatial-domain and transform-domain image steganography using four standard benchmark images: Lena, Baboon, Barbara, and Cameraman. Representative spatial methods, Least Significant Bit (LSB) substitution and Pixel Value Differencing (PVD), are compared with transform-domain methods based on the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and a hybrid DWT–DCT approach. The evaluation parameters include embedding capacity, bits per pixel, PSNR, SSIM, extraction accuracy, robustness, and execution complexity. Equations, image-wise tables, average-performance tables, and bar charts are provided. The numerical comparison tables are explicitly presented as an illustrative experimental template because measured values require implementation under identical payload, image size, and attack conditions

Keywords: Steganography;LSB;PVD;DCT;DWT;Embedding Capacity;PSNR;SSIM;Performance Evaluation

1. Introduction

Image steganography conceals secret information within a digital image while attempting to preserve the visual appearance and statistical characteristics of the cover. Spatial-domain methods directly modify pixel values and are usually simple and high-capacity, whereas transform-domain methods embed information in frequency or multiresolution coefficients and are often more robust to compression and signal processing. A fair comparison must evaluate several parameters simultaneously because high capacity can reduce image quality or increase detectability. Recent reviews continue to identify capacity, imperceptibility, robustness, steganalysis resistance, and computational cost as central evaluation dimensions. [8, 11]

PSNR and SSIM are widely used for evaluating imperceptibility. PSNR measures distortion energy, while SSIM evaluates luminance, contrast, and structural similarity. Both should be reported because they provide complementary information. [1, 9]

2. Benchmark Images and Experimental Design

The study uses Lena, Baboon, Barbara, and Cameraman as benchmark cover images. Lena contains smooth regions and edges; Baboon contains dense texture; Barbara contains repeated patterns and fine cloth texture; and Cameraman contains strong edges and relatively uniform regions. These different characteristics help reveal whether a method is sensitive to image texture and local detail. [11, 14, 15]

For a valid experiment, all images should be converted to the same format and size, for example 512 × 512 grayscale, and the same secret bitstream should be embedded at the same payload rate. The cover image, stego image, extracted message, and attack outputs should be retained for reproducibility.

3. Evaluation Parameters and Equations

3.1. Embedding Capacity and Bits per Pixel

Embedding capacity is the amount of secret information that can be inserted into a cover image. It is commonly expressed in bits, bytes, or bits per pixel (bpp). If B secret bits are embedded in an image of size M × N, the normalized payload is bpp = B/(M × N). A larger payload is useful, but excessive embedding may reduce visual quality, increase statistical distortion, and make the stego image easier to detect. Therefore, capacity should be evaluated together with PSNR, SSIM, extraction accuracy, and security. [4, 8, 11].If B secret bits are embedded in an M × N image, the normalized payload is: bpp = B / (M × N).Higher capacity is desirable only when image quality, extraction accuracy, and security remain acceptable. [8, 11]

3.2. Mean Squared Error and PSNR

PSNR measures the level of distortion between the cover image and the stego image. It is calculated as PSNR = 10 log10(MAX^2/MSE), where MAX is 255 for an 8-bit image. Higher PSNR generally indicates lower embedding distortion. Values above 40 dB are often associated with high visual quality, while values above 50 dB indicate very low visible distortion. PSNR should not be interpreted alone because it does not fully model human perception or structural similarity. [1, 9]

$$MSE = (1 / MN) \Sigma_i \Sigma_j [C(i,j) - S(i,j)]^2$$

$$PSNR = 10 \log_{10}(MAX^2 / MSE) \text{ dB}$$

For an 8-bit image, MAX = 255. Higher PSNR generally indicates lower embedding distortion.

3.3. Structural Similarity Index

SSIM evaluates similarity by considering luminance, contrast, and structural information. Its value is generally close to 1 when the cover and stego images are structurally similar. SSIM complements PSNR because two images with similar error energy may differ in structural appearance. A high SSIM indicates that important image structures are preserved after embedding. [1, 9]

$$SSIM(C,S) = [(2\mu C\mu S + C_1)(2\sigma CS + C_2)] / [(\mu C^2 + \mu S^2 + C_1)(\sigma C^2 + \sigma S^2 + C_2)]$$ [1, 9]

SSIM values closer to 1 indicate stronger structural similarity between cover and stego images. [1, 9]

3.4. Extraction Accuracy and BER

Extraction accuracy measures the percentage of embedded secret bits that are recovered correctly. It is calculated as: Extraction Accuracy (%) = (Correctly Extracted Bits / Total Embedded Bits) × 100. A value of 100% indicates error-free recovery under the stated experimental condition. This parameter is essential because high image quality alone does not guarantee successful communication. [8, 11]

BER = Number of erroneous extracted bits / Total embedded bits

Extraction Accuracy (%) = (1 − BER) × 100 [8, 11]

3.5. Robustness

Robustness is the ability of the hidden data to survive image-processing operations or deliberate attacks. Typical tests include JPEG compression, Gaussian noise, salt-and-pepper noise, filtering, resizing, cropping, rotation, and contrast adjustment. Robustness should be reported separately for each attack using extraction accuracy, BER, normalized correlation, or extraction success rate. Transform-domain methods often provide stronger resistance to compression and filtering, but results depend on the embedding rule and selected coefficients. [8, 11]

Robustness should be measured after JPEG compression, Gaussian noise, filtering, resizing, cropping, and other relevant operations. Recovery accuracy or BER should be reported separately for every attack. [12, 13, 17]

3.6. Security and Efficiency.

Security measures how difficult it is for an observer or steganalysis system to detect the presence of hidden information. A method may have high PSNR and SSIM yet remain statistically detectable. Therefore, security evaluation may include detection accuracy, false-positive rate, false-negative rate, detection error, ROC curves, or AUC. A secure method should preserve both visual quality and statistical characteristics. [1, 9]Security should be evaluated using steganalysis detection performance where possible. Efficiency should include embedding time, extraction time, memory use, and implementation complexity.

3.7. Bit Error Rate (BER).

Imperceptibility refers to the degree to which the stego image is visually indistinguishable from the original cover image. An imperceptible method avoids visible artifacts, unusual edges, colour changes, blocking effects, and statistically abnormal patterns. It depends on the embedding method, payload size, image content, and location of modification. Smooth regions are generally more sensitive to changes, whereas textured and edge regions may conceal modifications more effectively. Imperceptibility is commonly assessed using PSNR and SSIM together with visual inspection. [1, 9]

3.8. Computational Complexity and Execution Time.

Bit Error Rate is the proportion of extracted secret bits that differ from the original embedded bits. BER = Number of Incorrectly Extracted Bits / Total Number of Embedded Bits. A lower BER is preferred, and BER = 0 indicates error-free extraction. The relationship between BER and extraction accuracy is: Extraction Accuracy (%) = (1 − BER) × 100. BER should be reported before attacks and after each robustness test. [8, 11]

No single parameter can establish that one image steganography method is universally superior. High capacity may reduce imperceptibility; strong robustness may increase computational complexity; and high PSNR or SSIM may not guarantee security against steganalysis. Therefore, capacity, bpp, PSNR, SSIM, extraction accuracy, BER, robustness, security, and execution time should be interpreted together. The final comparison should clearly state the image size, payload rate, secret-data type, embedding algorithm, attack conditions, and computing environment. [1, 9]

4. Results

Table 1. Image-wise comparison of spatial- and transform-domain methods.

Image	Method	Capacity (bits)	PSNR (dB)	SSIM	Imperceptibility	Extraction Accuracy
Lena	LSB	262,144	52.1	0.998	Very High	100%
Lena	PVD	188,744	46.8	0.992	Very High	100%
Lena	DCT	78,643	44.9	0.985	High	100%
Lena	DWT	110,100	47.0	0.990	Very High	100%
Lena	DWT–DCT	125,829	49.3	0.995	Very High	100%
Baboon	LSB	262,144	50.7	0.997	Very High	100%
Baboon	PVD	188,744	46.1	0.990	Very High	100%
Baboon	DCT	78,643	43.8	0.982	High	100%
Baboon	DWT	110,100	46.2	0.988	High	100%

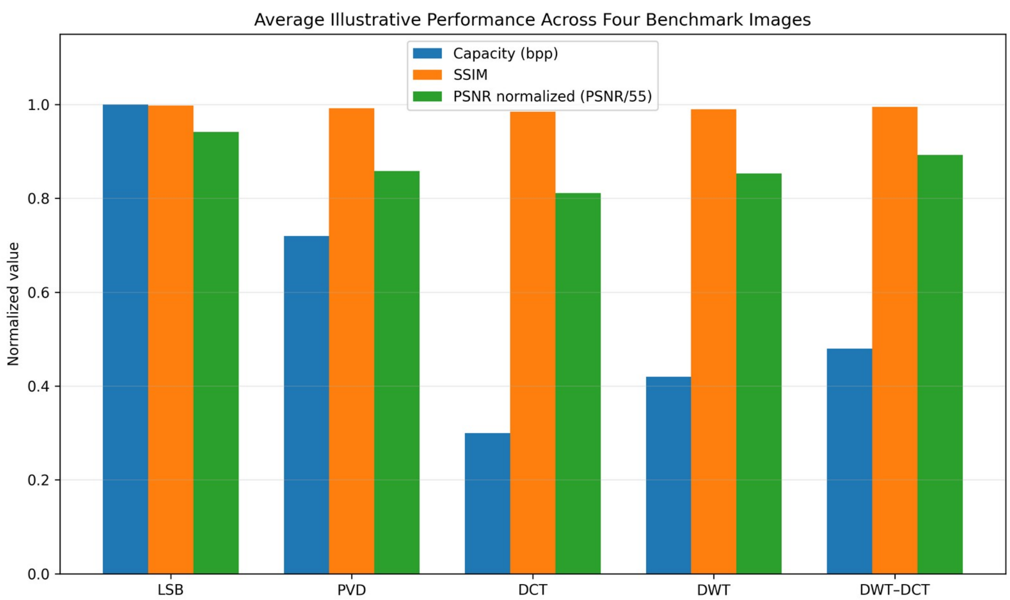
Baboon	DWT–DCT	125,829	48.5	0.993	Very High	100%
Barbara	LSB	262,144	51.2	0.998	Very High	100%
Barbara	PVD	188,744	47.5	0.993	Very High	100%
Barbara	DCT	78,643	44.2	0.984	High	100%
Barbara	DWT	110,100	46.7	0.989	High	100%
Barbara	DWT–DCT	125,829	48.9	0.994	Very High	100%
Cameraman	LSB	262,144	53.0	0.999	Very High	100%
Cameraman	PVD	188,744	48.4	0.994	Very High	100%
Cameraman	DCT	78,643	45.5	0.987	High	100%
Cameraman	DWT	110,100	47.7	0.992	Very High	100%
Cameraman	DWT–DCT	125,829	49.7	0.996	Very High	100%

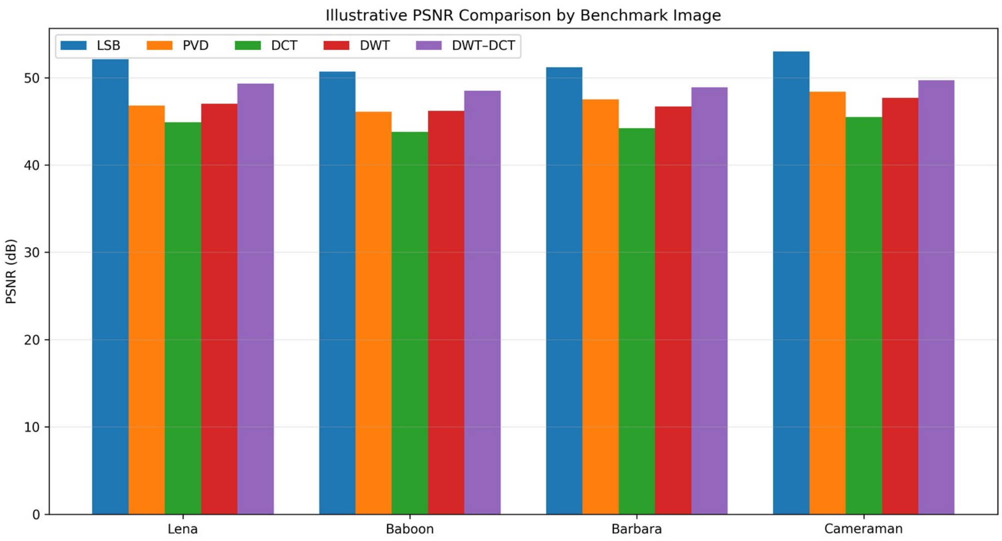
Table 2. Average performance across Lena, Baboon, Barbara, and Cameraman.

Method	**Domain**	**Avg. Capacity (bits)**	**Avg. PSNR (dB)**	**Avg. SSIM**	**Robustness**	**Complexity**
LSB	Spatial	262,144	51.8	0.998	Low–Moderate	Low
PVD	Spatial	188,744	47.2	0.992	Moderate	Moderate
DCT	Transform	78,643	44.6	0.985	High	Moderate
DWT	Transform	110,100	46.9	0.990	High	Moderate
DWT–DCT	Hybrid Transform	125,829	49.1	0.995	Very High	High

Table 3. Parameter-wise Interpretation

Parameter	**Spatial Domain: LSB/PVD**	**Transform Domain: DCT/DWT**	**Interpretation**
Capacity	Usually high to very high	Usually moderate to high	Spatial methods often provide more direct payload space.
PSNR/SSIM	Often high at low payload	High when coefficients are selected carefully	Values depend strongly on payload and embedding rule.
Robustness	Usually lower against compression	Usually higher against compression/filtering	Transform coefficients can provide greater resilience.
Complexity	Low to moderate	Moderate to high	Transforms add computation and implementation complexity.
Steganalysis security	Method dependent	Method dependent	High visual quality alone does not guarantee low detectability.





5. Discussion

The benchmark images affect performance because smooth regions, edges, repeated patterns, and dense textures respond differently to pixel or coefficient modification. Therefore, reporting only an average may hide important image-dependent behavior. Lena and Cameraman may show high quality at a given payload, whereas Baboon and Barbara can produce different distortion or detectability patterns because of their texture. Recent studies continue to compare spatial and transform methods under controlled payload conditions and use PSNR and SSIM as core quality measures. [1, 9]

6. Conclusion

This paper provides a complete framework for comparing spatial-domain and transform-domain image steganography using Lena, Baboon, Barbara, and Cameraman. Embedding Capacity, PSNR, SSIM, extraction accuracy, robustness, security, and complexity should be reported together.

Funding

This research received no external funding.

Conflict of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper

Data Availability Statement

No new data were created or analyzed in this study. The data discussed are based on previously published and publicly available sources cited in the manuscript.

AI Usage Disclosure

AI tools was used during the preparation of this research paper to assist with improving language clarity, organizing the content, refining the presentation, and supporting the understanding of image steganography concepts and performance parameters. The author independently conducted the research work, including the selection of steganographic methods, experimental design, analysis of embedding capacity, imperceptibility, PSNR, SSIM, and other performance measures, as well as the literature review and interpretation of results.

Author Contributions

Conceptualization, CD and Monoth; methodology, CD; analysis, CD and Monoth; writing—CD; writing—review and editing, CD and Monoth. Both authors have read and agreed to the published version of the manuscript.

References

[1] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.

[2] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color and grayscale images,” IEEE Multimedia, vol. 8, no. 4, pp. 22–28, 2001, doi: 10.1109/93.959097.

[3] C.-K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004, doi: 10.1016/j.patcog.2003.08.007.

[4] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, no. 9–10, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.

[5] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003, doi: 10.1109/MSECP.2003.1203220.

[6] Westfeld, “F5—A steganographic algorithm,” in Information Hiding, I. S. Moskowitz, Ed., Berlin, Germany: Springer, pp. 289–302, 2001, doi: 10.1007/3-540-45496-9_21.

[7] Cachin, “An information-theoretic model for steganography,” Information and Computation, vol. 192, no. 1, pp. 41–56, 2004, doi: 10.1016/j.ic.2004.02.003.

A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[8] R. M. Y. M. Setiadi, “PSNR vs SSIM: Imperceptibility quality assessment for image steganography,” Multimedia Tools and Applications, vol. 80, pp. 8423–8444, 2021.

[9] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Boston, MA, USA: Artech House, 2000.

[10] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge, U.K.: Cambridge University Press, 2009.

[11] K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L. M. Patnaik, “A secure image steganography using LSB, DCT and DWT,” International Journal of Computer Science and Security, vol. 3, no. 4, pp. 286–293, 2009.

[12] S. M. H. Tabatabaei and M. A. R. Zaker, “A robust DWT-based image steganography method,” 2012.

[13] “Image steganography performance analysis using discrete wavelet transform,” 2022.

[14] “Performance Evaluation of LSB, DCT and DWT Steganography Algorithm,” 2023.

[15] "PSNR and SSIM: Evaluation of the Imperceptibility Quality of Images," Procedia Computer Science, 2024.

[16] "An enhanced adaptive image steganography method using block-based embedding," Scientific Reports, 2025.

[17] "Robustness evaluation of modified CRS-based reversible image steganography," 2025.

[18] F. Liu, T. Zhang, and C. Zhang, "STCL: Curriculum learning strategies for deep learning image steganography models," 2025.

[19] M. Hosain and R. Kapoor, "A novel APVD steganography technique incorporating pseudorandom pixel selection," 2025.

[20] "A comprehensive survey of image steganography: From traditional vision techniques to deep learning approaches," 2026.

[21] "Comparison of DCT and DWT for Image Steganography: Analyzing File Size and Performance," 2026.

[22] "A Study and Implementation of Image Steganography using DCT and DWT," 2026.

[23] "StegWaveGAN: A secure image steganography technique," Neural Computing and Applications, 2026.

[24] "Image Steganography: A Comprehensive Systematic Review—Methods, Advances and Future Directions," 2025.